UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA,

Plaintiff,

v.

TWITTER, INC., a corporation,

Defendant.

Case No. 3:22-cv-3070

STIPULATED ORDER FOR CIVIL PENALTY, MONETARY JUDGMENT, AND INJUNCTIVE RELIEF

STIPULATED ORDER FOR CIVIL PENALTY, MONETARY JUDGMENT, AND INJUNCTIVE RELIEF

The United States of America, acting upon notification and authorization to the Attorney General by the Federal Trade Commission ("Commission" or "FTC"), filed its Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief ("Complaint") in this matter pursuant to Sections 5(a) and (*l*), 13(b), and 16(a)(1) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §§ 45(a) and (*l*), 53(b), and 56(a)(1). Defendant has waived service of the summons and the Complaint. Plaintiff and Defendant stipulate to the entry of this Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief ("Stipulated Order") to resolve the claims for civil penalties and injunctive relief set forth in the Complaint.

THEREFORE, IT IS ORDERED as follows:

FINDINGS

1. This Court has jurisdiction over the subject matter and all of the parties.

2. Venue is proper as to all parties in this District.

3. The Complaint states a claim upon which relief may be granted against Defendant under Sections 5(a) and (*l*), 13(b), and 16(a)(1) of the FTC Act, 15 U.S.C. §§ 45(a), 45(*l*), 53(b), and

56(a)(1), including for violations of Part I of the Commission's Decision and Order in *In re Twitter, Inc.*, C-4316, 151 FTC LEXIS 162 (F.T.C. Mar. 2, 2011).

4. Defendant's activities are "in or affecting commerce," as defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

5. Defendant waives any claim that it may have under the Equal Access to Justice Act, 28 U.S.C. § 2412, concerning the prosecution of this action through the date of this Stipulated Order, and agrees to bear its own costs and attorney's fees.

6. Defendant neither admits nor denies any of the allegations in the Complaint, except as specifically stated in the Decision and Order set forth in Attachment A. Only for purposes of this action, Defendant admits the facts necessary to establish jurisdiction.

7. Defendant and Plaintiff waive all rights to appeal or otherwise challenge or contest the validity of this Stipulated Order.

I. MONETARY JUDGMENT FOR CIVIL PENALTY

IT IS FURTHER ORDERED that:

A. Judgment in the amount of ONE HUNDRED FIFTY MILLION dollars ($150,000,000.00) is entered in favor of Plaintiff against Defendant as a civil penalty pursuant to Section 5(*l*) of the FTC Act, 15 U.S.C. § 45(*l*).

B. Defendant is ordered to pay to Plaintiff, by making payment to the Treasurer of the United States, ONE HUNDRED FIFTY MILLION dollars ($150,000,000.00), which, as Defendant stipulates, its undersigned counsel holds in escrow for no purpose other than payment to Plaintiff. Such payment must be made within seven (7) days of entry of this Stipulated Order by electronic fund transfer in accordance with instructions specified by a representative of Plaintiff.

C. In the event of any default in payment, the entire unpaid amount, together with interest, as computed pursuant to 28 U.S.C. § 1961 from the date of default to the date of payment, shall immediately become due and payable.

D. Defendant relinquishes dominion and all legal and equitable right, title, and interest to all funds paid pursuant to this Stipulated Order. Defendant shall make no claim to or demand for return of the funds, directly or indirectly, through counsel or otherwise.

E. Defendant agrees that the facts alleged in the Complaint will be taken as true, without further proof, only in any subsequent civil litigation by Plaintiff to enforce its rights to any payment or monetary judgment pursuant to this Stipulated Order.

F. Defendant acknowledges that its Taxpayer Identification Numbers (Social Security Numbers or Employer Identification Numbers), which Defendant has previously submitted to Plaintiff, may be used for collecting and reporting on any delinquent amount arising out of this Stipulated Order, in accordance with 31 U.S.C. § 7701.

II. MODIFICATION OF DECISION AND ORDER

IT IS FURTHER ORDERED that Defendant, and its successors and assigns, shall consent to: (i) reopening of the proceeding in FTC Docket No. C-4316; (ii) waiver of its rights under the show cause procedures set forth in Section 3.72(b) of the Commission's Rules of Practice, 16 C.F.R. § 3.72(b); and (iii) modifying the Decision and Order in *In re Twitter, Inc.*, C-4316, 151 FTC LEXIS 162 (F.T.C. Mar. 2, 2011), with the Decision and Order set forth in Attachment A.

III. ADDITIONAL PROVISIONS

IT IS FURTHER ORDERED that Defendant shall provide to the Department of Justice copies of all of the reports, assessments, notifications, certifications, and other documents required or requested under the Decision and Order set forth in Attachment A as follows: Parts VI.A, VI.E, VIII.A, IX, X.A, XI.A, and XI.B. Such documents shall be furnished via email to Consumer.Compliance@usdoj.gov, with the subject line "United States v. Twitter, Inc., DJ 102-4022." In the event that electronic mail is unavailable, the documents may be sent to the Director of the Department of Justice's Consumer Protection Branch, and whomever he or she designates, via overnight courier (not the U.S. Postal Service) to: Director, Consumer Protection Branch, Department of Justice, 450 Fifth St. NW Ste. 6400-South, Washington, DC 20001, with the

subject line "United States v. Twitter, Inc., DJ 102-4022." Defendant agrees that the Department of Justice shall have the same rights as the Commission (as given in the Decision and Order set forth in Attachment A) to request such documents under the specified parts, subject to any applicable law or regulation. Within fourteen (14) days of receipt of a written request from a representative of the Department of Justice's Consumer Protection Branch related to the reports, assessments, notifications, certifications, and other documents produced pursuant to the parts of the Decision and Order identified in this paragraph, Defendant agrees to submit additional compliance reports or other requested information, which must be sworn under penalty of perjury. For purposes of this paragraph, "Defendant" shall have the same definition and scope as the definition of "Respondent" in Paragraph E on page 3 of the Decision and Order set forth in Attachment A.

IV. CONTINUING JURISDICTION

IT IS FURTHER ORDERED that this Court shall retain jurisdiction in this matter for purposes of construction, modification, and enforcement of this Stipulated Order.

SO ORDERED this ____ day of _____, 2022.

_____
UNITED STATES DISTRICT JUDGE

Dated: _____, 2022

SO STIPULATED AND AGREED:

Dated: May 25, 2022

FOR PLAINTIFF:

THE UNITED STATES OF AMERICA:

BRIAN M. BOYNTON
Principal Deputy Assistant Attorney General
Civil Division

ARUN G. RAO
Deputy Assistant Attorney General

GUSTAV W. EYLER
Director
Consumer Protection Branch

LISA K. HSIAO
Assistant Director

/s/ Zachary L. Cowan
ZACHARY L. COWAN
DEBORAH S. SOHN
Trial Attorneys
U.S. Department of Justice
Civil Division
Consumer Protection Branch
450 5th Street NW, Suite 6400-S
Washington, DC 20530
Telephone: (202) 451-7468
Zachary.L.Cowan@usdoj.gov
Deborah.S.Sohn@usdoj.gov

STEPHANIE M. HINDS
United States Attorney

MICHELLE LO
Chief, Civil Division

SHARANYA MOHAN
EMMET P. ONG
Assistant United States Attorneys
Northern District of California
450 Golden Gate Avenue
San Francisco, California 94102
Tel: (415) 436-7198
sharanya.mohan@usdoj.gov
emmet.ong@usdoj.gov

Dated: May 24, 2022

FOR THE FEDERAL TRADE COMMISSION:

JAMES A. KOHM
Associate Director
Division of Enforcement

LAURA KOSS
Assistant Director
Division of Enforcement

REENAH L. KIM
Attorney
Division of Enforcement

ANDREA V. ARIAS
Attorney
Division of Privacy and Identity Protection

Federal Trade Commission
600 Pennsylvania Avenue, N.W.,
Mail Stop CC-9528
Washington, D.C. 20580
Tel: (202) 326-2272 (Kim); -2715 (Arias)
rkim1@ftcgov; aarias@ftc.gov

FOR DEFENDANT TWITTER, INC.

Dated: 05/18/22

DAMIEN KIERAN
Chief Privacy Officer
Twitter, Inc.

Dated: 5/20/2022

LYDIA B. PARNES
Wilson Sonsoni Goodrich & Rosati
1700 K Street N.W., Fifth Floor
Washington, D.C. 20006
Tel: (202) 973-8800
lparnes@wsgr.com

Counsel for Twitter, Inc.

ATTACHMENT A

202-3062

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Lina M. Khan, Chair**
Noah Joshua Phillips
Rebecca Kelly Slaughter
Christine S. Wilson

In the Matter of	**DECISION AND ORDER**
TWITTER, INC., *a corporation.*	**Docket No. C-4316**

DECISION

The Federal Trade Commission ("Commission") initiated an investigation of certain acts and practices of the Respondent named in the caption. The Commission's Bureau of Consumer Protection ("BCP") prepared and furnished to Respondent a draft Complaint. BCP proposed presenting the draft Complaint to the Commission. If issued, the draft Complaint would charge Respondent with violations of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §§ 45(a)(1) and (*l*), 53(b), and 56(a)(1).

Respondent neither admits nor denies any of the allegations in the Complaint, except as specifically stated in the Decision and Order. Only for purposes of this action, Respondent admits the facts necessary to establish jurisdiction.

The Commission considered the matter and determined that it had reason to believe Respondent has violated the Decision and Order the Commission previously issued in *In re Twitter, Inc.*, C-4316, 151 FTC LEXIS 162 (F.T.C. March 2, 2011) and the FTC Act, and that a Complaint should issue stating its charges in that respect. After due consideration, the Commission issues the Complaint, makes the following Findings, and issues the following Order:

FINDINGS

1. Respondent Twitter, Inc. ("Twitter") is a Delaware corporation with its principal office or place of business at 1355 Market Street, Suite 900, San Francisco, CA 94103.

2. The Commission has jurisdiction over the subject matter of this proceeding and over the Respondent, and the proceeding is in the public interest.

3. The Complaint charges violations of Section 5 of the FTC Act, 15 U.S.C. § 45, and violations of Provision I of an order previously issued by the Commission, 15 U.S.C. § 56(a)(1).

4. Respondent waives any claim that it may have under the Equal Access to Justice Act, 28 U.S.C. § 2412, concerning the prosecution of this action through the date of this Order, and agrees to bear its own costs and attorney fees.

5. Respondent and the Commission waive all rights to appeal or otherwise challenge or contest the validity of this Order.

ORDER

DEFINITIONS

For the purpose of this Order, the following definitions apply:

A. "**Covered Incident**" means any instance affecting 250 or more Users in which: (1) any United States federal, state, or local law or regulation requires Respondent to notify any U.S. federal, state, or local government entity that information collected or received, directly or indirectly, by Respondent from or about an individual consumer was, or is reasonably believed to have been, accessed or acquired without authorization; or (2) individually identifiable Covered Information collected or received, directly or indirectly, by Respondent, was, or is reasonably believed to have been, accessed, acquired, or publicly exposed without authorization. "Covered Incident" does not include instances where the only unauthorized access, acquisition, or exposure was due to a User communicating through Respondent's services (e.g., public tweets, protected tweets, retweets, or direct messages) information that was obtained from sources other than Respondent.

B. "**Covered Information**" means information from or about an individual consumer including, but not limited to: (1) a first or last name; (2) geolocation information sufficient to identify a street name and name of city or town; (3) an email address or other online contact information, such as an instant messaging User identifier or a screen name; (4) a mobile or other telephone number; (5) photos and videos; (6) Internet Protocol ("IP") address, User ID, or other persistent identifier that can be used to recognize a User over time and across different devices, websites, or online services; (7) a Social Security number; (8) a driver's license or other government issued identification number; (9) financial account number; (10) credit or debit information; (11) date of birth; (12) biometric information; or (13) any information combined with any of (1) through (12) above. "Covered Information" does not include information that a User intends to make public using Respondent's services.

C. "**Representatives**" means Respondent's officers, agents, servants, employees, attorneys, and those persons in active concert or participation with them who receive actual notice of this Order by personal service or otherwise.

D. "**Resources**" means networks, systems, and software.

E. "**Respondent**" means Twitter, Inc. ("Twitter"), and its successors and assigns. For purposes of Parts V and VI, Respondent means Twitter, Inc., its successors and assigns, and any business that Respondent controls directly or indirectly, except for any business that: (1) does not provide services that are offered to U.S. residents; or (2) does not collect, maintain, use, disclose, access, or provide access to the Covered Information of U.S. residents to enable Respondent's microblogging, social networking, or communications services.

F. "**Timeline Notice**" means a message Respondent places in a User's Twitter timeline (*i.e.*, the main screen the User sees when opening Twitter which displays a stream of tweets from accounts the User has chosen to follow) that stays near the top (*i.e.*, within the first five (5) tweets) of a User's Twitter timeline: (1) for at least six (6) months from the effective date of the Order; (2) until the User clicks on the "Learn More about your options" button embedded in the message; or (3) until the User scrolls past the message in their timeline, whichever occurs earlier.

G. "**User**" means an identified individual from whom Respondent has obtained information for the purpose of providing access to Respondent's products and services.

I. PROHIBITION AGAINST MISREPRESENTATIONS

IT IS ORDERED that Respondent and its Representatives, directly or through any corporation, subsidiary, division, website, mobile app, or other device, in connection with the offering of any product or service in or affecting commerce, must not misrepresent, in any manner, expressly or by implication, the extent to which Respondent maintains and protects the privacy, security, confidentiality, or integrity of Covered Information, including, but not limited to, misrepresentations related to:

A. Respondent's privacy and security measures to prevent unauthorized access to Covered Information;

B. Respondent's privacy and security measures to honor the privacy choices exercised by Users;

C. Respondent's collection, maintenance, use, disclosure, or deletion of Covered Information;

D. The extent to which a User can control the privacy of any Covered Information maintained by Respondent, and the steps a User must take to implement such controls;

E. The extent to which Respondent makes or has made Covered Information accessible to any third parties;

F. The extent to which Respondent targets advertisements to Users or enables third parties to target advertisements to Users; or

G. The extent to which Respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy or security program sponsored by a government or any self-regulatory or standard-setting organization, including but not limited to

the EU-U.S. Privacy Shield framework, the Swiss-U.S. Privacy Shield framework, and the APEC Cross-Border Privacy Rules.

II. LIMITATIONS ON USE OF TELEPHONE NUMBERS OR EMAIL ADDRESSES SPECIFICALLY PROVIDED TO ENABLE ACCOUNT SECURITY FEATURES

IT IS FURTHER ORDERED that Respondent and its Representatives must not use, provide access to, or disclose, for the purpose of serving advertisements, any telephone number or email address obtained from a User before the effective date of this Order for the purpose of enabling an account security feature (*e.g.*, two-factor authentication, password recovery, re-authentication after detection of suspicious or malicious activity). Nothing in Provision II will limit Respondent's ability to use, provide access to, or disclose such telephone numbers or email addresses if obtained separate and apart from a User enabling such account security feature and in a manner consistent with the requirements of this Order.

III. REQUIRED NOTICE TO CONSUMERS

IT IS FURTHER ORDERED that, within fourteen (14) days after the effective date of this Order, Respondent must provide a Timeline Notice to all current U.S. Users who joined Twitter prior to September 17, 2019, that states: "**Twitter's Use of Your Personal Information for Tailored Advertising** As we stated on Oct. 8, 2019, we may have served you targeted ads based on an email address or phone number you provided to us to secure your account.", and includes a "Learn more about your options" button that links to a webpage showing the information in Exhibit A.

IV. REQUIRED MULTI-FACTOR AUTHENTICATION OPTIONS

IT IS FURTHER ORDERED that, as of the effective date of this Order, Respondent must allow Users to utilize multi-factor authentication without providing a telephone number to access their Twitter accounts, such as by integrating authentication applications or allowing the use of security keys. The Company may use equivalent, widely-adopted industry authentication options that do not require Users to provide a telephone number and that are not multi-factor, if the person or persons responsible for the Program under Provision V.C: (1) approve(s) in writing the use of such equivalent authentication options; and (2) document(s) a written explanation of how the authentication options are widely-adopted and at least equivalent to the security provided by multi-factor authentication.

V. MANDATED PRIVACY AND INFORMATION SECURITY PROGRAM

IT IS FURTHER ORDERED that Respondent, in connection with the collection, maintenance, use, disclosure of, or provision of access to Covered Information, must, within one hundred eighty (180) days of issuance of this Order, establish and implement, and thereafter maintain a comprehensive privacy and information security program (the "Program") that protects the privacy, security, confidentiality, and integrity of such Covered Information. To satisfy this requirement, Respondent must at a minimum:

A. Document in writing the content, implementation, and maintenance of the Program;

B. Provide the written program, and any evaluations thereof or updates thereto to Respondent's board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer of Respondent responsible for the Program at least once every calendar quarter;

C. Designate a qualified employee or employees to coordinate and be responsible for the Program;

D. Assess and document, at least once every twelve (12) months and promptly following the resolution of a Covered Incident (not to exceed ninety 90 days after the discovery of the Covered Incident), internal and external risks to the privacy, security, confidentiality, or integrity of Covered Information that could result in the: (1) unauthorized collection, maintenance, use, disclosure, alteration, destruction of, or provision of access to Covered Information; or the (2) misuse, loss, theft, or other compromise of such information;

E. Design, implement, maintain, and document safeguards that control for the material internal and external risks Respondent identifies to the privacy, security, confidentiality, or integrity of Covered Information identified in response to Provision V.D. Each safeguard must be based on the volume and sensitivity of Covered Information that is at risk, and the likelihood that the risk could be realized and result in the: (1) unauthorized collection, maintenance, use, disclosure, alteration, or destruction of, or provision of access to Covered Information; or the (2) misuse, loss, theft, or other compromise of such information. Such safeguards must also include:

1. Prior to implementing any new or modified product, service, or practice that collects, maintains, uses, discloses, or provides access to Covered Information, conducting an assessment of the risks to the privacy, security, confidentiality, or integrity of the Covered Information;

2. For each new or modified product, service, or practice that does not pose a material risk to the privacy, security, confidentiality, or integrity of Covered Information, documenting a description of each reviewed product, service, or practice and why such product, service, or practice does not pose such a material risk;

3. For each new or modified product, service, or practice that poses a material risk to the privacy, security, confidentiality, or integrity of Covered Information, conducting a privacy review and producing a written report ("Privacy Review") for each such new or modified product, service, or practice. The Privacy Review must:

(a) Describe how the product, service, or practice will collect, maintain, use, disclose, or provide access to Covered Information, and for how long;

(b) Identify and describe the types of Covered Information the product, service, or practice will collect, maintain, use, disclose, or provide access to;

(c) If the Covered Information will be collected from a User, describe the context of the interaction in which Respondent will collect such Covered Information (*e.g.*, under security settings, in pop-up messages in the timeline, or in response to a prompt reading, "Get Better Ads!");

(d) Describe any notice that Respondent will provide Users about the collection, maintenance, use, disclosure, or provision of access to the Covered Information;

(e) State whether and how Respondent will obtain consent from Users for the collection, maintenance, use, disclosure, or provision of access to Covered Information;

(f) Identify any privacy controls that will be provided to Users relevant to the collection, maintenance, use, disclosure, or provision of access to the Covered Information;

(g) Identify any third parties to whom Respondent will disclose or provide access to the Covered Information;

(h) Assess and describe the material risks to the privacy, security, confidentiality, and integrity of Covered Information presented by the product, service, or practice;

(i) Assess and describe the safeguards to control for the identified risks, and whether any additional safeguards need to be implemented to control for such risks;

(j) Explain the reasons why Respondent deems the notice and consent mechanisms described in Provisions V.E.3(d) and V.E.3(e) sufficient;

(k) Identify and describe any limitations on the collection, maintenance, use, disclosure, or provision of access to Covered Information based on: (i) the context of the collection of such Covered Information; (ii) notice to Users; and (iii) any consent given by Users at the time of collection or through subsequent authorization;

(l) Identify and describe any changes in how privacy and security-related options will be presented to Users, and describe the means and results of any testing Respondent performed in considering such changes, including but not limited to A/B testing, engagement optimization, or other testing to evaluate a User's movement through a privacy or security-related pathway;

(m) Include any other safeguards or other procedures that would mitigate the identified risks to the privacy, security, confidentiality, and integrity of Covered Information that were not implemented, and each reason that such alternatives were not implemented; and

(n) Include any decision or recommendation made as a result of the review (*e.g.*, whether the practice was approved, approved contingent upon safeguards or other recommendations being implemented, or rejected);

4. Safeguards to prevent the collection, maintenance, use, disclosure, or access to Covered Information beyond the limitations identified in Provision V.E.3(k), including:

(a) Regular training, at least once a year, for any employees and independent contractors whose responsibilities include the collection, maintenance, disclosure, use, or provision of access to Covered Information, on the permissible collection, maintenance, disclosure, use, or provision of access to Covered Information and any related limitations;

(b) Written attestations by those employees and independent contractors that they will not collect, maintain, disclose, use, or provide access to the Covered Information in a manner inconsistent with those limitations;

(c) Designation of a senior officer, or senior level team composed of no more than five (5) persons, to be responsible for any decision to collect, maintain, use, disclose, or provide access to the Covered Information; and

(d) Treating any new method of collecting, maintaining, using, disclosing, providing access to, or deleting the Covered Information as a new or modified product, service, or practice requiring the reviews set forth in Provisions V.E.1-3;

5. Regular privacy and information security training programs for all employees and independent contractors on at least an annual basis, updated to address any identified material internal or external risks and safeguards implemented pursuant to this Order;

6. Technical measures to monitor Respondent's Resources to identify unauthorized attempts to: (a) access, modify, or exfiltrate Covered Information from Respondent's Resources; or (b) access or take over Users' accounts; and

7. Data access policies and controls for all: (a) databases storing Covered Information; (b) Resources that provide access to Users' accounts; and (c) Resources containing information that enables or facilitates access to Respondent's internal network and systems;

F. Assess, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following the resolution of a Covered Incident, the sufficiency of any safeguards in place to address the internal and external risks to the privacy, security, confidentiality, or integrity of Covered Information, and modify the Program based on the results;

G. Test and monitor the effectiveness of the safeguards at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following the resolution of a Covered Incident, and modify the Program based on the results. Such testing and monitoring must include: (1) vulnerability testing of Respondent's network(s) once every four (4) months and promptly (not to exceed thirty (30) days) after an unauthorized intrusion into Respondent's Resources; and (2) penetration testing of Respondent's network(s) at least once every twelve (12) months and promptly (not to exceed thirty (30) days) after an unauthorized intrusion into Respondent's Resources;

H. Select and retain service providers capable of safeguarding Covered Information they access through or receive from Respondent, and contractually require service providers to implement and maintain safeguards sufficient to address the internal and external risks to the privacy, security, confidentiality, or integrity of Covered Information; and

I. Evaluate and adjust the Program in light of any changes to Respondent's operations or business arrangements, a Covered Incident, new or more efficient technological or operational methods to control for the risks identified in Provision V.D of this Order, or any other circumstances that Respondent knows or has reason to believe may have an impact on the effectiveness of the Program or any of its individual safeguards. At a minimum, Respondent must evaluate the Program at least once every twelve (12) months and modify the Program based on the results.

VI. INDEPENDENT PROGRAM ASSESSMENTS BY A THIRD PARTY

IT IS FURTHER ORDERED that, in connection with compliance with Provision V of this Order titled Mandated Privacy and Information Security Program, Respondent must obtain initial and biennial assessments ("Assessments"):

A. The Assessments must be obtained from one or more qualified, objective, independent third-party professionals ("Assessor(s)") who: (1) use procedures and standards generally accepted in the profession; (2) conduct an independent review of the Program; (3) retain all documents relevant to each Assessment for five (5) years after completion of such Assessment; and (4) will provide such documents to the Commission within ten (10) days of receipt of a written request from a representative of the Commission. No documents relating to Respondent's compliance with this Order may be withheld from the Commission by the Assessor on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney-client privilege, statutory exemption, or any similar claim. Respondent may obtain separate assessments for (1) privacy and (2) information security from multiple Assessors, so long as each of the Assessors meets the qualifications set forth above;

B. For each Assessment, Respondent must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name, affiliation, and qualifications of the proposed Assessor, whom the Associate Director shall have the authority to approve in her or his sole discretion;

C. The reporting period for the Assessments must cover: (1) the first three-hundred-and-sixty-five (365) days after the issuance date of the Order for the initial Assessment; and (2) each two-year period thereafter for twenty (20) years after issuance of the Order for the biennial Assessments;

D. Each Assessment must, for the entire assessment period: (1) determine whether Respondent has implemented and maintained the Program required by Provision V of this Order, titled Mandated Privacy and Information Security Program; (2) assess the effectiveness of Respondent's implementation and maintenance of Provisions V.A-I; (3) identify any gaps or weaknesses in, or instances of material noncompliance with, the Program; (4) address the status of gaps or weaknesses in, or instances of material non-compliance with, the Program that were

identified in any prior Assessment required by this Order; and (5) identify specific evidence (including, but not limited to, documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is: (a) appropriate for assessing an enterprise of Respondent's size, complexity, and risk profile; and (b) sufficient to justify the Assessor's findings. No finding of any Assessment shall rely primarily on assertions or attestations by Respondent's management. The Assessment must be signed by the Assessor, state that the Assessor conducted an independent review of the Program and did not rely primarily on assertions or attestations by Respondent's management. To the extent that Respondent revises, updates, or adds one or more safeguards required under Provision V.E of this Order during an Assessment period, the Assessment must assess the effectiveness of the revised, updated, or added safeguard(s) for the time period in which it was in effect, and provide a separate statement detailing the basis for each revised, updated, or additional safeguard; and

E. Each Assessment must be completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, Respondent must submit the initial Assessment to the Commission within ten (10) days after the Assessment has been completed via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re Twitter, Inc., FTC File No. 202-3062." All subsequent biennial Assessments must be retained by Respondent until the Order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request.

VII. COOPERATION WITH THIRD-PARTY ASSESSOR(S)

IT IS FURTHER ORDERED that Respondent and its Representatives, whether acting directly or indirectly, in connection with any Assessment required by Provision VI of this Order titled Independent Program Assessments by a Third Party, must:

A. Provide or otherwise make available to the Assessor all information and material in their possession, custody, or control that is relevant to the Assessment for which there is no reasonable claim of privilege;

B. Provide or otherwise make available to the Assessor information about Respondent's Resources(s) and all of Respondent's IT assets so that the Assessor can determine the scope of the Assessment, and have visibility to Resource(s) and IT assets deemed in scope; and

C. Disclose all material facts to the Assessor(s), and not misrepresent in any manner, expressly or by implication, any fact material to the Assessor's: (1) determination of whether Respondent has implemented and maintained the Program required by Provision V of this Order, titled Mandated Privacy and Information Security Program; (2) assessment of the effectiveness of the implementation and maintenance of Provisions V.A-I; or (3) identification of any gaps or weaknesses in, or instances of material noncompliance with, the Program.

VIII. CERTIFICATIONS

IT IS FURTHER ORDERED that Respondent must:

A. One year after the issuance date of this Order, and each year thereafter, provide the Commission with a certification from a senior corporate manager, or, if no such senior corporate manager exists, a senior officer of Respondent responsible for the Program that: (1) Respondent has established, implemented, and maintained the requirements of this Order; (2) Respondent is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission; and (3) includes a brief description of all Covered Incidents during the certified period. The certification must be based on the personal knowledge of the senior corporate manager, senior officer, or subject matter experts upon whom the senior corporate manager or senior officer reasonably relies in making the certification; and

B. Unless otherwise directed by a Commission representative in writing, submit all annual certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re Twitter, Inc., FTC File No. 202-3062."

IX. COVERED INCIDENT REPORTS

IT IS FURTHER ORDERED that Respondent, within thirty (30) days after Respondent's discovery of a Covered Incident, must submit a report to the Commission. The report must include, to the extent possible:

A. The date, estimated date, or estimated date range when the Covered Incident occurred;

B. A description of the facts relating to the Covered Incident, including the causes of the Covered Incident, if known;

C. A description of each type of Covered Information that was affected or triggered any notification obligation to the U.S. federal, state, or local government entity;

D. The number of Users whose Covered Information was affected or triggered any notification obligation to the U.S. federal, state, or local government entity;

E. The acts that Respondent has taken to date to remediate the Covered Incident and protect Covered Information from further exposure or access, and protect affected individuals from identity theft or other harm that may result from the Covered Incident; and

F. A representative copy of any materially different notice sent by Respondent to consumers or to any U.S. federal, state, or local government entity.

Unless otherwise directed by a Commission representative in writing, all Covered Incident reports to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, NW,

Washington, DC 20580. The subject line must begin, "*In re Twitter, Inc.*, FTC File No. 202-3062."

X. ORDER ACKNOWLEDGMENTS

IT IS FURTHER ORDERED that Respondent obtain acknowledgments of receipt of this Order:

A. Respondent, within ten (10) days after the effective date of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.

B. For five (5) years after the issuance date of this Order, Respondent must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees having managerial responsibilities relating to the subject matter of this Order, and all agents and representatives who participate in any acts or practices subject to this Order; and (3) any business entity resulting from any change in structure as set forth in the Provision titled Compliance Report and Notices. Delivery must occur within ten (10) days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.

C. From each individual or entity to which Respondent delivered a copy of this Order, Respondent must obtain, within thirty (30) days, a signed and dated acknowledgment of receipt of this Order, which can be obtained electronically.

XI. COMPLIANCE REPORTING AND NOTICES

IT IS FURTHER ORDERED that Respondent makes timely submissions to the Commission:

A. Two-hundred and forty (240) days after the issuance date of this Order, Respondent must submit a compliance report, sworn under penalty of perjury, in which Respondent: (1) identifies the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission may use to communicate with Respondent; (2) identifies all of Respondent's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (3) describes the activities of each business, including the goods and services offered and the means of advertising, marketing, and sales; (4) describes in detail whether and how Respondent is in compliance with each Provision of this Order; and (5) provides a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.

B. Respondent must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any change in the following: (1) any designated point of contact; (2) the structure of Respondent or any entity that Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order; (3) the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against Respondent.

C. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: "I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____" and supplying the date, signatory's full name, title (if applicable), and signature.

D. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: "In re Twitter, Inc., FTC File No. 202-3062."

XII. RECORDKEEPING

IT IS FURTHER ORDERED that Respondent must create certain records for twenty (20) years after the issuance date of the Order, and retain each such record for five (5) years. Specifically, Respondent must create and retain the following records:

A. Accounting records showing the revenues from all goods or services sold;

B. Personnel records showing, for each person that Respondent contracts with directly and that provides services in relation to any aspect of the Order, whether as an employee or otherwise, that person's: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;

C. Copies or records of all U.S. consumer complaints concerning the subject matter of the Order, and any responses to such complaints;

D. A copy of each unique advertisement or other marketing material making a representation subject to this Order;

E. A copy of each widely-disseminated representation by Respondent or its Representatives that describe the extent to which Respondent maintains and protects the privacy, security, confidentiality, or integrity of Covered Information, including, but not limited to, (1) statements relating to any change in any product, service, or practice that relates to the privacy, security, confidentiality, or integrity of such information, and (2) statements relating to: (a) Respondent's privacy and security measures to prevent unauthorized access to Covered Information; (b) Respondent's privacy and security measures to honor the privacy choices exercised by Users; (c) Respondent's collection, maintenance, use, disclosure, or deletion of Covered Information; (d) the extent to which a User can control the privacy of any Covered Information maintained by Respondent, and the steps a User must take to implement such controls; (e) the extent to which Respondent makes or has made Covered Information accessible to any third parties; (f) the extent to which Respondent allows third parties to serve advertisements to Users; or (g) the extent to which Respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy or security program sponsored by a government or any self-regulatory or standard-setting organization, including but not limited to the EU-U.S. Privacy Shield framework, the Swiss-U.S. Privacy Shield framework, and the APEC Cross-Border Privacy Rules;

F. All materials relied upon in making the statements in Provisions XII.D and XII.E, and copies of each materially different notice provided to Users and mechanisms for obtaining a User's consent for the collection, use, or disclosure of Covered Information (including screenshots/screencasts and User interfaces, consent flows, and paths a User must take to reach such settings);

G. All materials relied upon to prepare the Assessment, whether prepared by or on behalf of Respondent, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning Respondent's compliance with related Provisions of this Order, for the compliance period covered by such Assessment;

H. For 5 years from the date received, copies of all subpoenas, information provided in response to such subpoenas, and all material correspondence with law enforcement, if such communication relate to Respondent's compliance with this Order;

I. For 5 years from the date created or received, all records, whether prepared by or on behalf of Respondent, that contradict, qualify, or call into question Respondent's compliance with this Order; and

J. All records necessary to demonstrate full compliance with each Provision of this Order, including all submissions to the Commission.

XIII. COMPLIANCE MONITORING

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondent's compliance with this Order:

A. Within fourteen (14) days of receipt of a written request from a representative of the Commission, Respondent must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury; appear for depositions; and produce records for inspection and copying. The Commission is also authorized to obtain discovery, without further leave of court, using any of the procedures prescribed by Federal Rules of Civil Procedure 29, 30 (including telephonic depositions), 31, 33, 34, 36, 45, and 69.

B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with Respondent. Respondent must permit representatives of the Commission to interview anyone affiliated with Respondent who has agreed to such an interview. The interviewee may have counsel present.

C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondent or any individual or entity affiliated with Respondent, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

XIV. ORDER EFFECTIVE DATES

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate twenty (20) years from the date of its issuance (which date may be stated at the end of this Order, near the Commission's seal), or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however,* that the filing of such a complaint will not affect the duration of:

A. Any Provision in this Order that terminates in less than twenty (20) years;

B. This Order if such complaint is filed after the Order has terminated pursuant to this Provision.

Provided, further, that if such complaint is dismissed or a federal court rules that Respondent did not violate any Provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

April J. Tabor
Secretary

SEAL:
ISSUED:

Exhibit A to
Attachment A

EXHIBIT A

[To appear with the Twitter logo and Twitter's standard website header]

We may have asked for your phone number or email address to secure or authenticate your account (for example, for two-factor authentication). As we told you in October 2019, we may have used these phone numbers or email addresses to deliver tailored advertising to you on Twitter until September 2019. On [date], we entered into a settlement with the Federal Trade Commission to resolve this issue.

As of September 17, 2019, we are no longer using phone numbers or email addresses collected for safety or security purposes for advertising. We never disclosed or shared your phone number or email address with advertisers. There is no action that you need to take regarding this issue.

You have a number of options to control your privacy and security when you use Twitter:

- **Control your privacy settings.** You can find out more about your privacy settings on Twitter, including how to enable or disable personalized ads, by visiting https://myprivacy.twitter.com.

- **Review your multi-factor authentication settings.** By requiring both a password and a secondary code or security key to access your account, multi-factor authentication can help keep your account safe. You can use an authentication app, a security key, or a phone number for multi-factor authentication. (And if you provide us a phone number for multi-factor authentication, it will not be used for advertising purposes without your consent.) You can learn about multi-factor authentication settings by visiting https://help.twitter.com/en/managing-your-account/two-factor-authentication.

For more details about how we protect the information you share with us and how we use that data, we encourage you to visit the Twitter Privacy Center.

We are very sorry this happened. If you have questions or comments about this notice or what we do to protect your information moving forward, you may contact Twitter's Office of Data Protection through this form.

[To appear with the Twitter's standard website footer]

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of **TWITTER, Inc.,** ***a corporation.***	**Docket No. C-4316**

DECISION

The Federal Trade Commission ("Commission") issued a Decision and Order against Twitter, Inc. ("Twitter) in Docket C-4316 on March 2, 2011 ("2011 order").[1] On [INSERT DATE], the United States of America, acting upon notification and authorization to the Attorney General by the Commission, filed a complaint ("2022 complaint") in federal district court alleging that Twitter violated the 2011 order by misrepresenting the extent to which it maintained and protected the privacy of nonpublic consumer information. The complaint also alleged that Twitter violated Section 5 of the FTC Act by misrepresenting how it would use telephone numbers and email addresses that users provided to enable a security feature.

On [INSERT DATE], Judge [INSERT JUDGE'S NAME] in the District for the Northern District of California entered a Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief ("Stipulated Order") resolving the 2022 complaint. In Section II of the Stipulated Order, Twitter consented to: (1) reopening the 2011 proceeding in FTC Docket No. C-4316; (2) waiving its rights under the show cause procedures set forth in Section 3.72(b) of the Commission's Rules of Practice, 16 C.F.R. § 3.72(b); and (3) modifying the 2011 Order with the new Decision and Order set forth below.

In view of the foregoing, the Commission has determined that it is in the public interest to reopen the proceeding in Docket No. C-4316 pursuant to Commission Rule 3.72(b), 16 C.F.R. § 3.72(b), and to issue a new order as set forth below. Accordingly,

IT IS ORDERED that this matter be, and it hereby is, reopened; and

IT IS FURTHER ORDERED that, Twitter having consented to modifying the 2011 order as set forth below, the Commission hereby modifies the 2011 order with the attached Decision and Order.

[1] *In the Matter of Twitter, Inc.*, C-4316, 151 FTC LEXIS 162 (F.T.C. March 2, 2011).